MOBILE DEVICE SECURITY—EMERGING THREATS, ESSENTIAL STRATEGIES

Key Capabilities for Safeguarding Mobile Devices and Corporate Assets

Table of Contents

Table of Figures

Executive Summary

In the past few years, the market adoption and utility of mobile devices has expanded dramatically. Yet for every positive development in this market, there is often a corollary risk. For example, while application stores give users unprecedented ease of access to a plethora of programs, they are also proving to be a fertile environment for the distribution of malware. Also, the increased power of mobile devices makes them more suitable for a host of business purposes, which can also result in the exposure and compromise of corporate data and systems. Finally, the very portability of mobile devices means that they are highly susceptible to loss and theft. This paper examines the threats to which mobile devices are currently exposed, and it describes the key strategies organizations need to employ in order to guard against these threats.

Introduction

Today, smartphones and other mobile devices are playing an increasingly central role in how people are entertained, communicate, network, work, bank, and shop.

Advancements within the mobile market—whether in performance, storage, applications, or capabilities—have been occurring at a dizzying pace. However, there is a fundamental area in which broad advancements have not been realized on mobile devices, particularly when compared to the personal computer, and that area is security. While mature security software such as antivirus is ubiquitous on laptops and desktops, the vast majority of mobile devices today remain completely devoid of security protection.

Not surprisingly, today's mobile devices—and the corporate assets they may connect to—are vulnerable. The following sections outline the threats currently plaguing mobile devices.

Threats to Mobile Devices, Users, and Corporate Assets

Malware

Mobile Devices at Risk

- Criminals using PC-style malware attacks to infect mobile devices.
- Greatest mobile malware risk comes from rapid proliferation of apps in application stores.

Given the lack of security mechanisms employed, and the increased proliferation and power of mobile devices, it is no surprise that malware is proliferating. Between 2009 and 2010, there was a reported increase in threats of 250%[1]. Virtually all major platforms are malware targets. Examples include trojans that send short message service (SMS) messages to premium rate numbers, background calling applications that rack up exorbitant long distance bills for victims, keylogging applications that can compromise passwords, self propagating code that infects devices and spreads to additional devices listed in the address book, and more. Further, these threats continue to grow more sophisticated, with polymorphic attacks—malware that changes characteristics during propagation to avoid detection—now being perpetrated.

Spyware applications have also been prevalent. These applications monitor device communications and often can be remotely controlled by cyber criminals. Commercial spyware applications—such as FlexiSpy (**www.flexispy.com**), Mobile Spy (**www.mobile-spy.com**), and MobiStealth (**www.mobistealth.com**)—are readily available and effective at concealing their presence from the user of an infected device. This spyware can typically only be detected by robust mobile anti-malware products. These spyware applications enable an attacker to monitor SMS and Multimedia Messaging Service (MMS) messages, emails, inbound and outbound call logs, and user locations. They can even allow an attacker to remotely listen to phone conversations. Compounding matters is that, if these spyware applications compromise mobile devices that are used for business, they can pose a great risk to the confidentiality, integrity, and availability of corporate data.

While commercial spyware applications are nothing new to mobile security experts, the rapid proliferation of programs available via various application stores perhaps poses the greatest malware threat moving forward. Designed as a means to allow even entry-level developers to create and distribute applications, application stores pose a significant risk—providing an ideal mechanism for delivering malicious software to high volumes of mobile devices.

[1]Information obtained from analysis of Juniper Networks Junos Pulse Mobile Security Suite virus definition database dated 10/15/2010

In 2010, a bank phishing application targeting mobile phones was discovered[2]. A developer published a program that purported to be an application for accessing online bank accounts. After users installed the application, they were presented with the bank's URL and were prompted for their login credentials. After login credentials were submitted, these details were then shipped off to an unknown location, presumably for fraudulent activities.

In that same year, another highly publicized attack took place. A device manufacturer was found to be shipping devices with Secure Digital (SD) cards preloaded with the Mariposa botnet, which affected personal computers[3]. When the user unpacked the new device and connected it via USB cable to a PC, the SD card's autorun function would initiate the botnet and infect the user's computer.

Loss and Theft

The portability of mobile devices allows for continuous access to business and personal information, regardless of location. This portability also leads to the very common incidence of loss or theft of mobile devices. In fact, one survey of consumer users found that one out of every three users has lost their device[4] at some point in time.

These lost devices can present a plethora of devastating consequences. Not only is the device at risk, but bookmarked bank accounts with passwords set to auto-complete in the browser, contacts with pictures and addresses tied to the contact, calendar events, social media accounts, personal photos, pre-connected email accounts, and other data can also be jeopardized.

Further, because people are using their mobile devices for work related functions, the loss of a mobile device can also present devastating business implications, exposing intellectual property, sensitive employee and customer information, and a host of other corporate assets.

Communication Interception

Communication interception is a threat to any device that connects to a network, and mobile devices are no exception. The advantage that smartphones have is that their communications are often encrypted over cell networks, requiring would-be hackers to have specialized equipment and tools to listen to the conversations between the device and cell towers. However, this encryption can be broken and the methodology to do so is well documented and publicly available.

Further, the Wi-Fi connections of smartphones also pose a communication interception threat. With approximately 50% of all smartphones currently containing Wi-Fi capabilities, and a projected 90% of devices having this functionality by 2014[5], the risk of Wi-Fi sniffing and interception is an increasingly prevalent risk.

Studies have shown that once a mobile device switches to a Wi-Fi network, it is susceptible to man-in-the-middle (MITM) attacks[6]. MITM is a method in which attackers introduce themselves into a communication stream. In essence, the attacker plays "middle man" for a conversation, logging all of the information that is being relayed between the communicating parties. The tools to conduct a MITM attack are widely available and the methodologies well documented.

Depending upon how a particular smartphone handles data transmissions, communications between two parties may be transmitted in clear text, and thus would be visible to an attacker using MITM methods. Figure 1 provides an example of an email sent by a smartphone over Wi-Fi and intercepted by a network monitoring tool.

[2]http://www.phonearena.com/htmls/Malicious-banking-app-found-in-the-Android-Marketplace-article-a_8744.html
[3]http://isc.sans.edu/diary.html?storyid=8389
[4]Information obtained from Junos Pulse Mobile Security Suite internal transaction logs
[5]http://www.wi-fi.org/news_articles.php?f=media_news&news_id=969
[6]http://threatcenter.smobilesystems.com/?p=1587

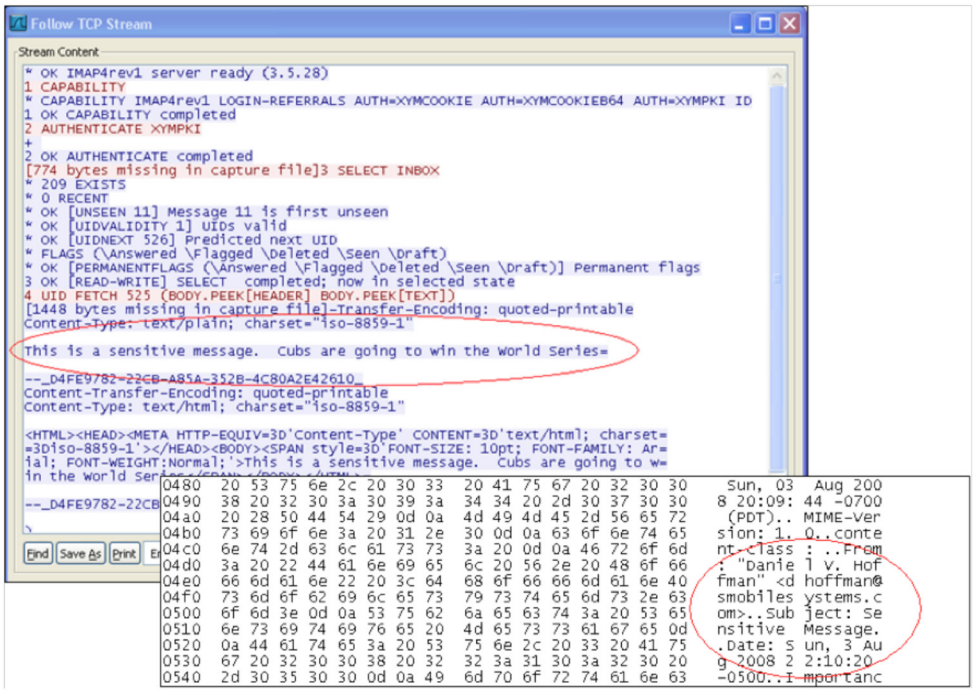

Figure 1. Example of an intercepted message sent by a smartphone

Exploitation and Misconduct

As with many different areas within security, the human element plays a predominant role in mobile device security. The same threats of exploitation and misconduct that apply to corporate and personal computer users also apply to users of mobile devices. Further, employees and teenagers typically have 24/7 access to mobile devices, which can exacerbate the threats posed.

One such threat is cyberbullying. In 2004, the Cyberbullying Research Center was established to study and report on the dangers that children face from their peers while they are online. One of the notable studies reported that cell phones are the most popular technological device that teens use, with 83% of teens using one at least weekly[7].

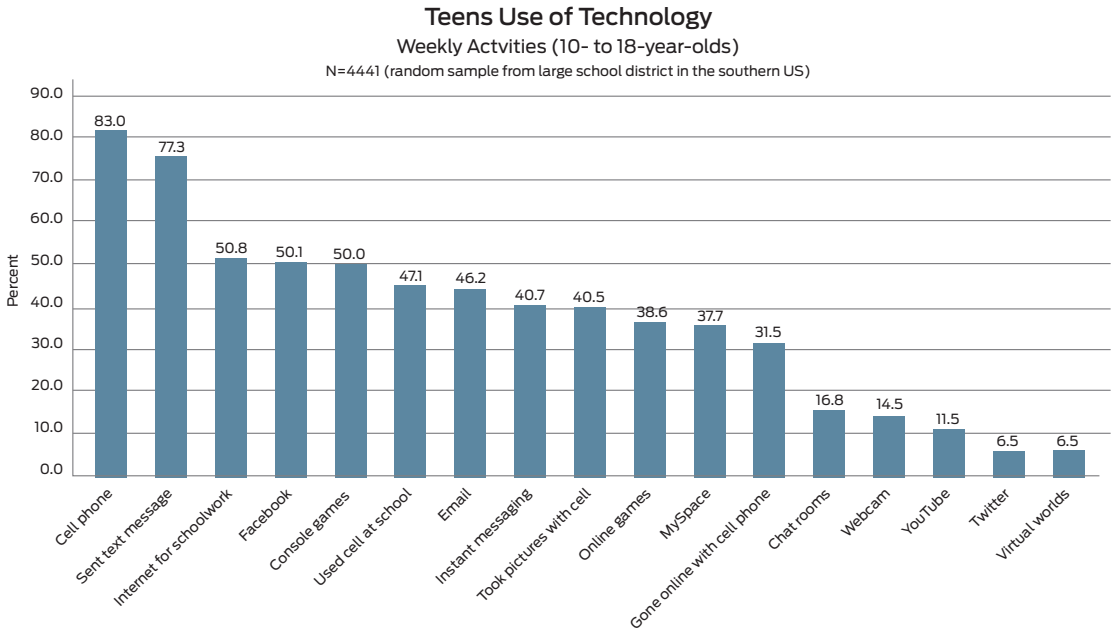

Figure 2. Teen technology use (Source: Cyberbullying Research Center)

[7]http://www.cyberbullying.us/research.php

Mobile phones and the social media tools that teens often use with mobile devices represent a fertile environment for teens to be bullied and harassed by their peers. In fact, 20.8% of all teens surveyed report that they have experienced bullying in one form or another[8].

In addition to cyberbullying, teens are also using their mobile devices for "sexting." Studies show that 20% of all teens have sent nude or semi-nude pictures or videos of themselves from their phones. 39% of teens are sending suggestive messages via SMS. Further, 29% of teens sending sexually suggestive content to someone from their mobile phone report sending it to someone that they say they only know online or have never met at all. 44% of teens also freely admit that it is common practice for sexually suggestive content to be shared with individuals other than the intended target[9].

The Strategic Imperative—Requirements for Addressing Today's Mobile Threats

Given the critical and pervasive nature of threats to mobile devices, organizations need several vital capabilities if they are to effectively and practically minimize their exposure:

- **Proactive malware protection.** Organizations need to protect mobile devices against malware and viruses delivered via email, SMS, MMS, direct download, Bluetooth, or infrared transmission. Security teams also need virus definition updates to be propagated to devices automatically. Further, mobile devices need capabilities for doing real-time scanning of incoming files and scans of internal memory, memory cards, and the entire device, as well as generating automated alerts if malware is detected.
- **Loss and theft protection.** To mitigate the risks posed by lost or stolen devices, users and IT administrators need cohesive, integrated mobile device management capabilities. This includes capabilities for using GPS to identify the precise location of a missing device. Organizations and individuals also need the assurance of remote backup so that data is available for immediate use if a device becomes inaccessible. Further, if a device is not retrieved, or an interim device needs to be employed, organizations should be able to restore data to any subsequent device, regardless of operating system. Finally, administrators need capabilities for remotely controlling devices, including initiating backups, locking, and removing sensitive data.
- **Safeguards against communication interception.** To guard against communication interception, IT teams need to employ VPNs that encrypt communications between mobile devices and corporate networks. Further, they need to establish and enforce corporate mobility policies, combining VPN access control with mobile security. This requires integration with an organization's laptop access mechanisms. Finally, if a threat or issue is detected that for any reason cannot be mitigated, security teams need capabilities for disabling the infected mobile device's access to prohibit further infection within the organization.

In addition, consumers should be able to turn to their service providers to gain device monitoring capabilities that can protect children from both cyberbullying and sexting, and alert parents in the event such behaviors occur.

Further, to effectively and efficiently employ these security mechanisms across large user communities, organizations need security solutions that offer the characteristics described below.

Broad Device and Mobile OS Support

Within a given organization, a number of mobile device operating systems are typically in use, and these must be factored into an organization's security framework. Further, this device support needs to go beyond smartphones. The reality is that smartphones, tablets, netbooks, and notebooks are complementary in nature. Typically, as consumers adopt a new device type, it won't signal the abandonment of any of their existing devices. For example, just because individuals purchase a new tablet doesn't mean that they will stop using their cell phone or laptop. The upshot of this is that security teams need to account for a broad set of devices, a set that gets larger with each passing day.

Particularly as the use of different device types and platforms grows, security administrators can't feasibly use a different management console for each mobile device platform or type, as this would prove more costly, inefficient, and susceptible to errors. Consequently, businesses need a single solution that can be used to manage all major operating systems, so that they can effectively, consistently, and efficiently apply security policies across each platform. For example, the same type of multi-factor authentication should be supported on all devices.

[8]http://www.cyberbullying.us/research.php
[9]http://www.pcsndreams.com/Pages/Sexting_Statistics.html

Integrated Mobile Device Management and Security Policy Enforcement

In addition to centralized control of disparate mobile device platforms and types, security administrators need capabilities that afford a centralized, cohesive means for doing both mobile device management and security policy enforcement. This includes the mobile device management capabilities outlined above such as remote locking and wiping of lost devices, as well as control of such security mechanisms as antivirus, personal firewalls, and more. Further, administrators need a unified management console that can support the following efforts:

- Establishing and enforcing corporate mobility policies, combining VPN access control with mobile security
- Enforcing granular, role-based access control to corporate applications
- Delivering seamless, cross-platform authentication for all users, regardless of their device

Minimal End User Requirements

In order to ensure that corporate security policies are strictly and consistently enforced, security teams need to be able to apply security policies that require minimal involvement or effort on the part of end users. The fewer responsibilities users have, the less susceptible devices will be to inconsistency and errors. Further, by minimizing any efforts or maintenance on the part of end users, enterprises can ensure optimal end user productivity, while at the same time minimizing the downtime and risks associated with compromised devices.

Leveraging Self-Help Models to Reduce IT Overhead

Security teams should leverage communities and online resources and reference materials to foster self-service capabilities for as many ongoing user requests as possible. For example, if users are looking to add a productivity application to their smartphone, IT can provide a categorized list of supported applications, instructions for installation, and even links for downloading. In addition, users can turn to communities to get questions answered and see how others are resolving similar issues. This approach can effectively empower users to solve problems themselves, while offloading significant distraction and effort from IT organizations with persistently constrained resources.

The Solution—Mobile Security from Juniper Networks

Juniper Networks provides the solutions and services that enable organizations and individuals to guard against the breadth of threats plaguing mobile devices today. Juniper solutions offer complete security capabilities, including proactive malware protection, mechanisms that guard against the damage of lost or stolen devices, and encryption of mobile device communications.

Further, by offering a complete, unified solution that features comprehensive OS and device support, minimal user requirements, integrated mobile device management and policy enforcement, and self-help support, Juniper provides an unrivaled combination of administrative efficiency, cost-effectiveness, and robust security.

Junos Pulse Mobile Security Suite

Juniper Networks® Junos® Pulse Mobile Security Suite is a comprehensive, scalable solution that provides smartphone security, management, and control. It protects mobile devices against malware, viruses, trojans, spyware, and other malicious attacks on most of today's leading mobile platforms and operating systems. The Mobile Security Suite also includes mobile device management features that mitigate the risk of losing or exposing corporate and personal data on devices that have been lost or stolen.

Junos Pulse Mobile Security Suite is enforced on mobile devices through the Junos Pulse client, which is free to users and available on such mobile platforms as Apple iOS, Google Android, Nokia Symbian, Windows Mobile, and BlackBerry. With the Junos Pulse Mobile Security Suite, individuals can continue to use all of their smartphone features while receiving nonintrusive, effective protection.

The Mobile Security Suite also includes the Junos Pulse Mobile Security Gateway management console, which offers comprehensive capabilities for configuring and managing mobile security policies. The Mobile Security Gateway is available as a hosted web-based console, simplifying deployment within an enterprise. The Mobile Security Gateway also provides detailed reports on virus infections, updates, and the latest threats detected on the mobile devices accessing the enterprise network.

Junos Pulse for Secure Connectivity

Junos Pulse is a single client that integrates intelligent, dynamic control over user access via Juniper Networks SA Series SSL VPN Appliances. At the same time, Junos Pulse dramatically simplifies the end user experience. With Pulse, end users no longer need to interact with network connectivity and security software. Instead, users simply supply their credentials and Pulse takes care of the rest. The IT staff is also able to reduce the number of software agents required and installed down to one, minimizing software conflicts and reducing deployment costs.

Juniper Global Threat Center

The Juniper Global Threat Center conducts around-the-clock security, vulnerability, and malware research tailored specifically to mobile device platforms and technologies. The Juniper Global Threat Center identifies, monitors, and responds to evolving threats affecting mobile devices, ensuring that Juniper customers always have the highest possible level of mobile device protection.

The center is staffed and managed by highly skilled experts with such certifications as Certified Information Systems Security Professionals (CISSP), Certified Ethical Hacker (CEH), and Certified Hacking Forensic Investigator (CHFI). The Juniper Global Threat Center brings proven, methodology-driven analysis of security to mobile environments—helping customers safeguard the confidentiality, integrity, and availability of mobile devices and corporate assets.

Conclusion

Threats to mobile devices are pervasive and escalating. Through malware, loss and theft, exploitation and misconduct, communication interception, and direct attacks, enterprises and users are increasingly susceptible to devastating compromises of mobile devices. With Juniper, organizations and individuals can cost-effectively guard against current and emerging threats, while retaining optimal productivity and flexibility in their use of mobile devices.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

2000372-001-EN Jan 2011 Printed on recycled paper